REPORT DOCUMENTATION PAGE	*Form Approved* **OMB No. 0704-0188**

1. REPORT DATE *(DD-MM-YYYY)* 23-03-2012	**2. REPORT TYPE** Master of Military Studies Research Paper	**3. DATES COVERED** *(From - To)* September 2011 - April 2012

4. TITLE AND SUBTITLE COMMUNICATIONS SECURITY: A TIMELESS REQUIREMENT WHILE CONDUCTING WARFARE	**5a. CONTRACT NUMBER** N/A
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER N/A
6. AUTHOR(S) MAJOR MICHAEL ANTHONY	**5d. PROJECT NUMBER** N/A
	5e. TASK NUMBER N/A
	5f. WORK UNIT NUMBER N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068	**8. PERFORMING ORGANIZATION REPORT NUMBER** N/A
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSOR/MONITOR'S ACRONYM(S)** N/A
	11. SPONSORING/MONITORING AGENCY REPORT NUMBER N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT

AS TECHNOLOGICAL ADVANCEMENTS IMPROVED THE MEANS BY WHICH COMMANDERS' COMMAND AND CONTROL ON THE BATTLEFIELD, COMMUNICATIONS SECURITY MUST REMAIN EVER PRESENT FOR MISSION SUCCESS. WARFIGHTERS ON EVERY LEVEL MUST FULLY PREPARE TO ADAPT COMMUNICATIONS SECURITY. ADDITIONALLY, TACTICS, TECHNIQUES, AND PROCEDURES SHOULD INCORPORATE COMMUNICATIONS SECURITY IN EVERY FACET ACROSS THE WARFIGHTING FUNCTIONS.

15. SUBJECT TERMS
COMMUNICATIONS SECURITY, COMSEC, INTELLIGENCE SECURITY

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT** UU	**18. NUMBER OF PAGES** 27	**19a. NAME OF RESPONSIBLE PERSON** Marine Corps University / Command and Staff College
a. REPORT Unclass	**b. ABSTRACT** Unclass	**c. THIS PAGE** Unclass			**19b. TELEPONE NUMBER** ***(Include area code)*** (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

COMMUNICATIONS SECURITY: A TIMELESS REQUIREMENT WHILE CONDUCTING WARFARE

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Michael Anthony

AY 11-12

Mentor and Oral Defense Committee Member: Craig A. Swanson, PhD
Approved:
Date: April 10, 2012

Oral Defense Committee Member: Brian S. Christmas, LTCOL USMC
Approved:
Date: 10 April 2012

Executive Summary

Title: Communications Security: A Timeless Requirement While Conducting Warfare

Author: Major Michael Anthony, United States Marine Corps

Thesis: As technological advancements improved the means by which commanders' command and control on the battlefield, communications security must remain ever present for mission success.

Discussion: Military battles require effective communications on every level, from seniors to subordinates, subordinates to seniors, and laterally. Communication is required to pass information, request support, coordinate events, and articulate desires between friends and foes. Because information is oftentimes sensitive, varying measures are often implemented to protect it from one degree to another. The role of signals or communications' intelligence during the battles of Pearl Harbor and Midway, along with the ongoing enigma, comprise valid and tangible examples of the importance of communications security. These examples exhibited success and failure for both America and its foes. Today's battlefield is no different and is potentially more vulnerable due to the proliferation of communication systems, their availability, and deliberated adversarial influences to compromise American systems.

Conclusion: Warfighters on every level must fully prepare to adapt communications security. Additionally, tactics, techniques, and procedures should incorporate communications security in every facet across the warfighting functions.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Illustrations

Page

Table of Contents

Preface

I undertook this research project to demonstrate the need for communications security across battlefields that continue to increase in both size and complexity and which we must operate seamlessly and effectively. Over the last decade information technology evolved so quickly that we as warriors often take the capabilities of these weapons, and our action or inaction toward them, for granted. More and more, computers and smart phones are becoming like side arms in our lives. Often we communicate with a simple text message or email rather than calling on the phone or visiting in the office. We rely greatly on video teleconferences when time and distance preclude ones ability to travel. Email, message traffic, and written orders or policy letters are the norm for passing information and coordination between seniors and subordinates. This information is very susceptible to interception and if discovered our enemies could use it to gain an advantage. As a result, we must be mindful and careful in all that we do as we never know who is watching and listening.

In order to stay within the unclassified realm, I limited my historical examples to the World War II era and made very little reference to information currently in use, which could give potential adversaries clues of past, current, or future capabilities. Additionally, if time were not a limitation, I would have liked to explore and expound upon examples in the European theater, such as the events surrounding the capturing of the German Engima machine and how the Allies exploited this information.

I would like to thank Dr. Swanson for his patience, mentoring, and guidance. I would also like to thank the staff at the National Cryptologic Museum for their assistance and time. Finally, I would like to thank a special friend all of their support.

> *Moreover, the vast area over which modern battles are fought, and the enormous number of men engaged, have made the task of direction of a great force impossible without more effective means of communication both of information and orders than was ever needed in the past.*[1]
>
> *George H. English, History of the 89th Division*

I. Introduction

Communication is a way of life. It is the means by which people relay information and enable others to understand their intentions. Communication occurs through various means, such as conversations, emails, letters, and phone calls, to name a few. Over time, the medium by which communication occurs has also evolved. Computers, personal digital assistants (PDA), and portable phones are but a few examples of how the world of communicating has evolved from analog radio communications to digital, high-speed devices. Along with the Internet, portable electronic devices have enhanced the reliability of communication, enabling constant and timely communications, and have erased the presumption that face-to-face communication is the most accurate and reliable form of communication. However, these electronic means of communicating have opened the door for a large number of vulnerabilities across the electromagnetic spectrum.

Because technology has evolved over time, the daily actions of all military members are required to change in order to protect American interests. What, if anything, needs to occur procedurally to ensure America’s foes are not granted access to sensitive or classified information due to poor practices or lack of accountability? Does the overreliance upon technology create a critical vulnerability within the military community that America’s foes can easily gain entry because military personnel lack the discipline with regards to communications security?

Communications security is important due to advancements in technology influences upon the speed, distance, scale, and potentially lethal nature of military daily actions and operations. Conversely, technology will continue to adapt new ways and means by which the military conducts business. Security of this information is paramount. Unauthorized access to information and the potential exploitation of both the information and the systems carrying the information pose significant issues to the military and national security. America "need[s] to protect our communications because they consistently reveal our strengths, weaknesses, disposition, plans, and intentions and if the opposition intercepts them he can exploit that information by attacking our weak points, avoiding our strengths, countering our plans, and frustrating our intentions . . . something he can only do if he has advance knowledge of our situation."[2] As technology continues to influence the ways by which the military operates, communications security will become increasingly important.

In times past, commanders relied upon messenger, signal light, flag semaphore, single channel radio, automated digital message traffic, and face-to-face conversation to relay information. Limited data could be transmitted via these methods, which were typically slow, lacked security, and oftentimes intercepted. Additionally, the time associated with delivery and supplemental actions lacked the effective response desired. Several inventions, such as the telephone and telegraph, were developed which directly impacted the ability whereby commanders could pass messages in a timely manner across the battlefield. As systems were created, the enemy soon adapted methods and procedures to compromise these systems.

As technological advancements improved the means by which a commander's command and control on the battlefield, communications security must remain ever present for mission success. Commanders have become accustomed to having access to various information systems. These range from video feeds, video teleconferences, secured voice communications, intelligence systems, and aggregated command and control systems such as the United States Army's Command Post of the Future (CPOF) program of record. Such capabilities require massive back-end support of manpower and equipment. Additionally, these systems often require fairly robust communication backbones with high data exchange rates.

The relevance of communications security on today's battlespace is of extreme importance. The means and methods of communicating are often tied to electronics and must be sent from one location to another. The information will traverse a radio wave or Ethernet cable. If this information is sent in the clear or plain text, the transmission may be easily intercepted. If this message is sent encrypted, the task of decrypting the message becomes a more challenging task for would be deciphers. Communications security remains relevant today because several of the means and methods of transmitting information in the past have been compromised or exploited thus rendering them ineffective. Both military and civilian organizations have developed solutions, both hardware and software, to protect information. Yet, at times, the human dynamic is the most vulnerable for protecting information.

The author of this essay desires to relay the importance of communications security to the reader. Communications security is a broad topic and many contributing factors affect the abilities of a determined enemy to compromise and exploit secrets. The military needs to take proper precautions to deny an enemy's ability to compromise and exploit systems. Although, this may seem benign or simple, communications security is a difficult task. Exploiting and compromising systems or encryption have great impacts on how military systems communicate. Additionally, the intelligence gained by exploitation could have deafening affects. Upon reading and digesting the information present, the reader will have examined the importance of communications security, historical examples of success and failures regarding communications security, the current issues within the military regarding communications security, and the future of communications security.

II. Communication

Communication is "the imparting or interchange of thoughts, opinions, or information by speech, writing, or signs."[3] Communications occur through various means. The military communicates tactically through field telephones, radios, messengers, computers, and visual signals such as flares, projectiles, smoke grenades, candles, signal flags, lights, hand signals, whistling arrows, and songs. Over time, the use of communicating has evolved as technology made various elements more fitting for different situations. Part of this evolution directly relates to the battlespace that the commanders organize for fighting. Areas of operation have increased greatly over time. As an example, the Pacific theater of operations during World War II spanned from the West Coast of the United States and Alaska south to Australia and west to China. Admiral Chester W. Nimitz, Commander-in-Chief Pacific Fleet, had to use communication systems to command and control his forces across the theater.[4]

Communication is necessary for commanders and staffs to understand what is happening to influence results on the battlefield. At the tactical level, a squad on patrol may need to request medical evacuation (MEDEVAC), air support, resupply, or transportation lift to move to another location on the battlefield. Another scenario on the battlefield may involve a commodore directing ships to conduct a blockade of a sea-lane. In either of these situations, the ability to relay the information in a timely and secure manner could have tremendous impact on the outcome of the commander's overall mission. In the case of the squad, eavesdropping may be an acceptable risk due to the short timeline associated with the request and the request being fulfilled. The time for the request to be fulfilled would occur prior to the enemy's ability to respond. The more obvious case requiring security is the blockade for several reasons. If a blockade were to be implemented, one could reasonably assume this would be an act of aggression, there would be some sort of opposition from those being denied access, and the potential for retaliation would be expected. No commander would want to openly tell his opponent his intentions and compromise the security of his force.

Communication is largely employed through three methods on the battlefield: voice (telephone and radio), data, and messenger.   Tactical telephones consist of traditional (or civilian) telephones that one may find in his or her own house. Used similarly to traditional telephones, tactical telephones are known as plain old telephone service (POTS) (see figure 1), non-secure telephones such as the TA-1042 (see figure 2) or Internet Protocol (IP) telephone (see figure 3), and secure telephones such as the KY-68 telephone (see figure 4) or Secure Terminal Equipment (STE) (see figure 5). These telephones generally connect to tactical switchboards that establish trunks to the Defense Information Systems Agency's (DISA) teleports granting access to military and commercial telephone networks. A trunk is a single circuit between two switching centers or individual message distribution points; in the aforementioned example the tactical network and the teleport.[5]

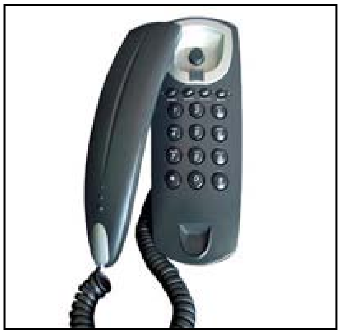

Figure 1

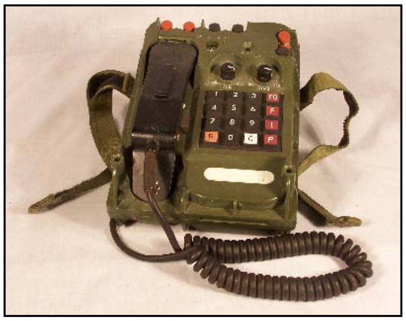

Figure 2

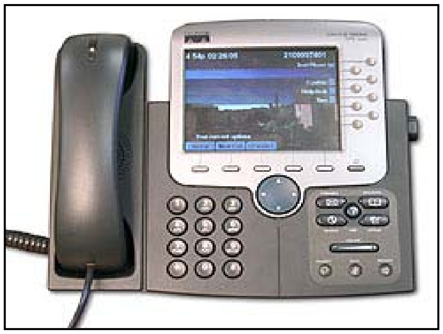

Figure 3

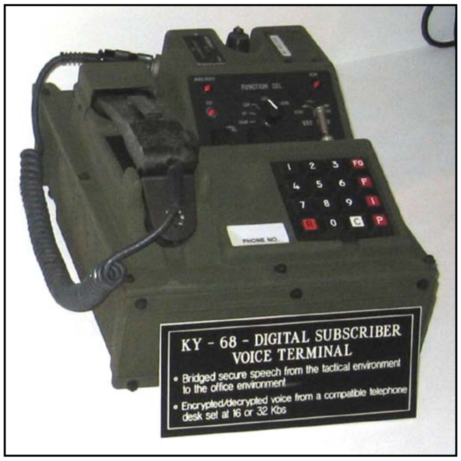
KY - 68 - DIGITAL SUBSCRIBER VOICE TERMINAL
• Bridged secure speech from the tactical environment to the office environment
• Encrypted/decrypted voice from a compatible telephone desk set at 16 or 32 Kbs
PHONE NO.
FUNCTION SEL

Figure 4

Figure 5

Radio communications come in two waveforms: amplitude modulation (long-range) and frequency modulation (short-range). Long-range communication is used for intra-theater, beyond line-of-sight, and over the horizon communications. This sort of communication is often used by units that are geographically separated or beyond line of sight with regards to the curvature of the earth's surface. Additionally, long-range radio communication is used for satellite communication between the ground station and the satellite. The atmosphere and bandwidth pose challenges to long-haul communications. High frequency (HF) communications must be thoroughly coordinated to minimize the atmospheric effects between daytime and nighttime operations. Satellite communication is limited by availability, the area for which it can transmit and receive data, and bandwidth. Short-range radio communication is often used by smaller units and for ground forces to communicate with air assets. An excellent example of a short-range radio is the man potable walkie-talkie that is often used in small, tactical environments, such as a squad on patrol. Both long-range and short-range radios are susceptible to jamming and interference thus proper measures should be taken to protect against such an attack or exploitation.

Although voice communications have the ability to cover long distances, these platforms do not have the ability to relay large amounts of information in the most expeditious manner. Therefore, systems to pass data communications across the battlefield are required. Data communications encompasses all electronic digital communications generally recognized by an email, website, server, and computer. Generally, tactical communications require units to establish Defense Information Service Network (DISN) services remotely to connect to the Global Information Grid (GIG). The GIG is the essential gateway to the Internet that DISA uses to allow service departments access. There are a host of routing protocols, name servers, and other services required to allow the system to work properly and as general users of the systems understand them to work normally.

Another very important and rapidly increasing technology using the data system is video teleconferencing. Video teleconferencing allows people, at multiple sites, geographically separated, to view one another while engaging in conversation. This allows the cognitive portion of our brains to capture visual cues during the video teleconference that is often missed while engaging in a phone conversation. Another capability of video teleconferencing is the projection of live video feeds, imagery, maps, PowerPoint briefs, and other visual aids that are used to relay information for an audience not co-located. The two basic models use IP technology and DISN Video Services-Global (DVSG) with IP being the most prominently used technology. The DVSG video teleconferencing requires a dedicated DISA circuit. As a result of this dedicated circuit requirement, most communication units opt not to use this method in order to conserve resources.

The last and oldest form of relaying information is via messenger. This method allows humans to deliver the intended message and is considered the most reliable means.[6] In practice, many commanders believed that this form of delivery provided a level of guarantee and if the message was not received, typically the messenger would give his life in its defense. The drawback of this method of delivery is that it is very susceptible to enemy interception and thus makes it vulnerable to interception and compromise.

As a result of having several ways of delivering information, security must be at the forefront of the criteria. The best means does not always translate into the most reliable or secure means of delivering information hence security must be the first criterion when determining what must occur. For example, if a commander needs to direct a unit to move to a different location for a time sensitive operation, the commander has several media to deliver this information, such as a telephone or email. If the commander decides the information is perishable and the risk of compromising the message is negated by time, the commander may place a non-secure telephone call to relay the information. Therefore, security is not always a requirement that many users of the equipment consider. However, information technology, intelligence, and operations professionals rely heavily on security. Of the means of relaying information previously detailed, the user has several options available with regards to security. On most tactical communication networks, both secure and non-secure means exist to relay information. Radio networks generally have covered and uncovered nets, for example, “Battalion Tac 1” would be covered and “Comm Coord” would be uncovered. Other examples are having non-secure POTSs and secure STEs for telephone resources and Nonsecure Internet Protocol Router Network (NIPRNET) as the unclassified data network and Secure Internet Protocol Router Network (SIPRNET) as the classified data network.

There are many ways to secure communication networks. Earlier practices of securing communication involved the substitution of letters, numbers, words, and ideas for something in its place like another word, number or picture. Cryptography is “the use of secret codes and ciphers to scramble information so that it’s worthless to anyone but the intended recipients.”[7] Encryption is the act of scrambling information into cipher text so that intercepted messages cannot be read.”[8] As technology improved, imaginative solutions, such as the Engima and the Navajo code, came along to assist people with securing information. Today, data encryption is used to navigate the Internet such as accessing one’s online bank account. Each of these capabilities and technologies has a direct correlation to communications security. World War II contains many examples of communications successes and failures; two of these examples will be explored in the next section.

III. Communication and its Security during World War II

Even before the United States’ involvement in World War II, communications security played a pivotal role in its success in the Pacific theater. Not only did the United States effectively use communications security for their advancement on the battlefield, likewise, the Japanese maintained a high level of communications security throughout its military forces to coordinate attacks and disguise their intentions. Although the United States suffered a devastating setback by the Japanese surprise attack on Pearl Harbor, the United States was able to quickly learn, adapt, and exploit the Japanese means of communicating which directly aided the United States’ success at the Battle of Midway only six months later. This portion of the essay will evaluate each of the aforementioned events to provide the reader a solid example of the relevance of communications security on the battlefield.

During the 1920s, the Director of Naval Intelligence reorganized the Office of Naval Intelligence and established a small section of cryptanalysts, OP-20-G, responsible for "obtaining official and commercial foreign radio traffic and exploiting the knowledge gained from decrypts."[9] As one might imagine, the task of decrypting messages is an arduous one. By 1940, the members of OP-20-G had an enormous workload and the Army's Signal Intelligence Service (a branch of the Army's Signal Corps) began to assist the Navy with this task. As both the Army and Navy cryptanalysts monitored the Japanese radio traffic, the cryptanalysts learned of three Japanese codes: Black code, Flag Officers Code-which was rarely used, and a five digit enciphered general purpose code JN-25-which became the aperiodic cipher used during World War II by the Imperial Japanese Navy (IJN). The JN-25 code required three books to operate: a code book (containing 30,000 five digit numbers), a book of random numbers (containing 300 pages of 10x10 number matrices), and an instruction book (containing the rules for the aperiodic cipher).[10]

In January 1941, American cryptanalyst successfully deciphered a portion of JN-25. The Japanese, however, released thousands of JN-25 encrypted messages between December 1940 and December 1941. Due to a lack of personnel and competing priorities the United States was not capable of deciphering all of these messages. At this time, the cryptanalysts' more pressing task was capturing, deciphering, and translating Japanese Diplomatic messages.[11] The Japanese took an additional step to secure their communications by using call signs. Call signs were given to battleships, cruisers, aircraft carriers, and locations. They were also changed frequently, even up to three weeks prior to their attack on Pearl Harbor.[12] Fleet Commander Admiral Isoroku Yamamoto led the Japanese attack organized into a Combined Fleet consisting of six battleships, two cruisers, and eight destroyers and a Pearl Harbor Strike Force consisting of two battleships, six aircraft carries, three cruisers, and sixteen destroyers.[13] Several conclusions have been drawn regarding why the United States failed to recognize the Japanese attack prior to it occurring.

Due to the controversies regarding whether or not leadership within the federal government had knowledge or should have had knowledge of the Japanese prior to 7 December 1941, there were eight investigations of the Pearl Harbor attack. The Department of the Navy conducted three investigations, the Department of War conducted three, the United States Supreme Court conducted one, and the United States Congress conducted one. The eight investigations were as follows:

The Roberts Commission, 18 December 1941 – 23 January 1942;
The Hart Inquiry, 12 February – 15 June1944;
The Army Pearl Harbor Board 20 July – 19 October 1944;
The Navy Pearl Harbor Court of Inquiry, 24 July – 19 October 1944;
The Clarke Investigation, 14-16 September 1944, 13 July – 4 August 1945;
The Clausen Investigation 23 November 1944 – 12 September 1945;
The Hewitt Inquiry, 14 May – 11 July 1945; and
The Joint Congressional Committee 15 November 1945 – 31 May 1946.

The Joint Congressional Committee investigation was the most thorough and incorporated findings from the previous seven.[14] The outcomes of these investigations determined that no one knew nor had actionable and timely intelligence prior to the attack.

The Japanese signal to launch the attack on Pearl Harbor was to be preceded by a "Winds Message." The message "East Wind Rain" identifies the Japanese intent to attack the United States; "North Wind Cloudy" identifies their intent to attack the Union of the Soviet Socialist Republics; and "West Wind Clear" identifies their intent to attack Great Britain. The Japanese were to alert their fleet and diplomatic posts, however, there were conflicting reports of when, or if, messages were received.[15] The Army Pearl Harbor Board and Navy Court of Inquiry investigations concluded the message was intercepted on 4 December 1941 and the intelligence staff of both departments were notified.[16] The Japanese exercised great discipline prior to the attack, which surprised the Americans. If the Japanese were not successful and the United States was able to capture, decipher, and translate the messages more timely, the United States could have been better prepared for the attacks. Preparation could have been accomplished by launching fighter aircraft, manning anti-aircraft guns, using torpedo nets, increased security and protection measures on ships such as watertight integrity, patrolling, and dispersed ships and aircraft throughout the region in order to ultimately thwart the Japanese attack.

At 0750 on 7 December 1941, the time of the Japanese attack, the United States had three aircraft carriers, eight battleships, seven light cruisers, and 21 destroyers in the vicinity of Pearl Harbor under the command of the Commander-in-Chief Pacific Command, Admiral Husband E. Kimmel.[17] Although significant American combat power was present in the vicinity of Pearl Harbor, American forces were not organized or prepared to respond to the Japanese attack in a robust manner.

After the Japanese attack on Pearl Harbor, the Battle of Midway was an example of America's success, which was enabled by communications security. The Japanese had more resources, experience, and creditability thus fostering their overconfidence and complacency in their communications security abilities and perceived accomplishments during the Battle of Coral Sea (7-8 May 1942), which preceded the Battle of Midway (3-8 June 1942).[18] In contrast, prior to and during the Battle of Midway, the Americans had the advantage as significant amounts of Japanese radio traffic were decoded. As American cryptanalysts continued to exploit significant portions of the JN-25 code, they were able to learn a great deal about Japanese intent, order of battle, tactics, techniques, and procedures in its Pacific campaign.[19] With this information, America was able to piece together information concerning Japanese fleet movement and their goal of expanding defensives in the Pacific.[20]

The Japanese attack plan at Midway was to bring the battle to American forces, draw out American carriers, and decisively defeat the American fleet at sea. The Japanese attack at Pearl

Harbor had damaged the United States inventory severely. The Untied States lost 2,403 service members and civilians and 1,178 wounded. Additionally, the United States lost all eight battleships (sunk or severely damaged), three cruisers were damaged, four destroyers were damaged, one minelayer sunk, two auxiliary ships sunk and one more severely damaged, and 169 aircraft destroyed and another 150 damaged.[21] It would take time to replenish the fleet. Foreseeing the need, President Franklin D. Roosevelt and Congress already approved the Two-Ocean Navy Act on19 July 1940.[22]

The 1941-1943 United States' fleet was significantly smaller than the Japanese in the Pacific. With expedited construction, two new fast battleships (USS *Washington* and USS *North Carolina*) were to be completed in 1941 along with six new *South Dakota* and *Iowa* class battleships under contract or scheduled to be built in 1942.[23] Nonetheless, the United States had three pre-World War II operations in the Pacific aircraft carriers (USS *Yorktown*, USS *Enterprise, and* USS *Hornet*) but no fast battleships in the Pacific capable of transiting at 25 knots or more and fighting along side the aircraft carriers for the Battle of Midway.[24, 25]

Due to the relative size of the United States Fleet, the cryptanalysts' ability to capture and decipher Japanese messages provided a huge advantage for the Americans during the Battle of Midway. Although all of the messages were not deciphered nor accurately interpreted once deciphered, the Americans were still able to learn many of the detailed Japanese plans and prepare its own counter attack by maximizing limited resources and placing them where they were needed the most. Prior to and during the Battle of Midway, the Japanese, once again under the leadership of Admiral Yamomoto, sought to battle the United States' Pacific Fleet away from the Hawaiian land-base air force and large garrison.[26] The Japanese plan was to capture the Midway Island and disperse the Combined Fleet in order to lure the Pacific Fleet into battle.

Once the Pacific Fleet committed to battle, the Combined Fleet would then attack the Pacific Fleet with massive amounts of aircraft, submarines, and battleships to defeat the Americans. This flawed planned led to the demise of the Combined Fleet.[27]

The Pacific Fleet Commander, Admiral Nimitz, anticipated a portion of the Japanese plan based on the information the cryptanalyst were able to obtain. Admiral Nimitz effectively ordered the Pacific Fleet into battle against Admiral Yamomoto's Combined Fleet. By positioning the Pacific Fleet and massing combat power, Admiral Nimitz was able to successfully use the aircraft carriers to launch aircraft which inflicted severe damage to the Combined Fleet.[28] At the end of fighting, the Americans defended Midway and decisively defeated the Japanese fleet. The United States suffered many losses, 307 were killed in action (KIA), the aircraft carrier USS *Yorktown*, one destroyer, and 147 aircraft, during the battle. The Japanese lost 2,500 KIA, four fast fleet carriers (among the best in the Japanese fleet), one heavy cruiser, and 332 aircraft.[29] Although the Japanese experienced significant material losses, the greatest loss was the quality pilots with extensive prewar training and combat experience in China during the first part of this war against the Allied forces as these pilots were irreplaceable for several years. The victory at the Battle of Midway occurred as a result of the hard work of cryptanalysts and their abilities to pass the information through to the proper channels for timely decisions to be made.

The Japanese attack on Pearl Harbor and the Battle of Midway are excellent examples of how communications security on the battlefield directly affected the element of surprise and enabled decisive victories. Admiral Yamomoto effectively commanded and controlled the Combined Fleet maintaining high levels of communications security and surprised the Americans on Pearl Harbor. The Japanese attack on Pearl Harbor propelled the United States into World War II and highlighted the necessity of the United States' ability to intercept and decipher enemy message while protecting its own. Although the Japanese's Combined Fleet had greater relative combat power than the United States' Pacific Fleet, the Combined Fleet was neutralized and defeated as Admiral Nimitz's forces were able to gain actionable intelligence prior to the Battle of Midway. The American success at Midway changed the tide of the war in the Pacific. Communications security validated its importance on the battlefield during World War II and for future conflicts.

IV. Communication and its Security on Today's Battlefield

Communication across today's battlefield is even more critical than in 1941 and 1942. Today's battlefield has expanded far beyond traditional domains of the sea, air, and land. Technology allows for speed and volume across the space and cyber domains to bring effects, not only on an opponent, but also on regions of the world while relying heavily on the use of the electromagnetic spectrum, global positioning satellites, Internet connectivity, and radios. As a result, securing communication is even more important.

This section identifies capabilities and threats the military faces as the threat environment evolved. Although the nature of warfare has not changed, in that it is the violent opposition of wills, the means by which it is waged has changed drastically. Several technological advancements occurred since the Battle of Midway, such as the advent of unmanned aircraft systems (UAS) and implementation of the command post of the future (CPOF), which were relied upon heavily throughout Operations Iraqi and Enduring Freedom.

The ease in which hostile actors can obtain weapons of mass destruction, chemical weapons, biological weapons, and bomb making materials is call for concern for nations that thrive off free market and global economies. These hostile actors, such as Al Qaida or Hezbollah, do not posses the requisite skill, armament, or capability to fight a linear battle with conventional forces such as the United States, United Kingdom, or Israel. Such a threat is not limited to non-state players. Conversely, violent state players such as Iran and North Korea seek to disrupt world events and threaten global stability.

The question remains, how can these states and non-state players accomplish their goals, achieve some level of success, and force the rest of the free world to defend and protect their interest? The answer is communication and its security on the battlefield. Except for a few places, such as Afghanistan, where the North Atlantic Treaty Organization (NATO) forces are engaged in combat operations with the Taliban, the preferred choice to wage battle for these violent players is in cyberspace. They utilize network systems to gain access, monitor, and exploit systems. Additionally, they leverage tools such as the media and social networking systems to publish their message, recruit followers, and organize attacks.

A recent example of a robust cyber attack occurred during the Russo-Georgia War in 2008. Although the cyber attacks originated in Russia, the attacks maneuvered across the world as a direct result of the complexity, nonlinear, and disjointed configuration of the cyber domain. Ultimately, the cyber attacks hit their intended Georgian targets, however, to date, no one has claimed responsibility for them. Many of these targets were identified, scoped out, and exploited several days prior to the air, ground, and sea attacks. The most significant exploits were targets against the government. The cyber attacks disrupted the daily operations of the government's ability to influence its people by compromising 54 websites that dealt with communications, finance, and government. It denied Georgian officials the ability to provide information to its people and the international community during the attack, as the attackers theoretically controlled the nation's media outlets. This synchronized cyber attack allowed the attackers to freely control the information and messaging being relayed both internally and externally. After the cyber attack was successfully disrupted nearly three weeks later the kinetic fight began.[30]

The Russo-Georgian example clearly identifies the potential capabilities the cyber domain brings to modern warfare. Hostile players thousands of miles away from one another may have the ability to deny, disrupt, defeat, or destroy targets that once were only an issue in a kinetic fight. The use of the electromagnetic spectrum and computer networks allow access to systems and resources that have regional and global effects. Communications security is the only way to guarantee American interests are not compromised. The American military continues to operate across the land, air, sea, and space domain. Technology has driven the cyber domain. Just as the military seeks to attain naval superiority and air supremacy it must now work diligently to obtain dominance in the cyber domain.

Another very alarming case illustrative of current communications security occurred during the 2006 Israel-Hezbollah War. During this war, the non-state player Hezbollah conducted combat operation for 34 days against the Israel Defense Force (IDF). Although the significance of a non-state player's ability to wage sustained combat operations against a formidable military causes great concern, of greater concern was their ability to conduct effective signals intelligence against an American ally. According to Mohamad Bazzi's article, a Hezbollah commander said, "We were able to monitor Israeli communications, and we used this to adjust our planning."[31]

If Hezbollah claims are true and they in fact did monitor Israeli single channel radio and telephone communications, then they were able to capture and de-encrypt signals. The Israeli government declined to confirm this accusation.[32] For tactical communications, the Israelis use a version of the American made Single Channel Ground and Airborne Radio System (SINCGARS) which has the ability to single channel plain text (clear), single channel cipher text, or frequency hopping. If the Israelis were operating in plain text then it is reasonable to assume their communication was compromised, as it was not secure. If they were operating in cipher text or frequency hopping, then how did Hezbollah intercept and subsequently crack the code? Does Hezbollah have the required skills, knowledge, and equipment to conduct sophisticated signals intelligence? Did another state or non-state actor assist Hezbollah or act on their behalf to compromise the signals? According to Bazzi, many believe Syria and Iran supported Hezbollah.[33] If another state assisted Hezbollah, where did they operate? The location is important because the SINCGARS family radio is generally a short-wave radio and has a range of about 25 miles with high power amplifiers and antennas.

The issues surrounding the telephone are similar to the challenges associated with exploiting and compromising single channel radios. If the Israeli telephone connections were unencrypted, a simple wiretap could have captured conversations. Additionally, if the Israelis relied upon cell phones for command and control, the ability to monitor these devices is relatively simple and could have easily been exploited. However, if the Israelis were using any sort of encryption devices, exploitation would have been difficult and the question remains, how was Hezbollah able to crack the code? Does this capability have impacts on the United States and the technologies used by the United States military?

The Department of Defense established the United States Cyber Command (USCYBERCOM) as a sub-unified command under the United States Strategic Command to combat potential cyber threats to the United States and its interest. Incidents like the Georgian and Israeli conflicts highlight the reason the United States created this organization. The cyber domain allows non-state actors global influence and the ability to cause damage politically, economically, and physically.   Therefore, the USCYBYERCOM's mission is as follows:

> USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries.[34]

The question of whether a cyber attack will affect the United States is no longer valid or the issue. Conversely, the questions are when will the next cyber attack occur, what will be the impact of the cyber attack, after the attack how long will the reconstruction process take, and how much will the attack cost in terms of money, resources, and technology setback.

V. Conclusion

Communications security has played a significant role in American military history. It is ever present on the battlefields and countless examples of its increased importance exist. Communication is required for commanders to exercise command and control. Technology on the battlefields continues to evolve and expand along with the areas of interest, influence, and operations. As technology evolves, the means by which information travels must also adapt. The logical evolution also occurs when attempting to capture and exploit new technologies.

History on the battlefield depicts commanders and staffs exchanging information while enemies attempt to intercept information to gain an advantage. The information exchanged has occurred across the spectrum from live person voice to telephone to single channel radio to video conferencing and from hand written messages to automated message. Computer command and control system platforms, such as Command Post of the Future, have replaced maps and map pens. Several military commands and supporting organizations, such as the United States Cyber

Command and the National Security Agency, have also evolved to assist battlefield commanders with protecting their information and capturing enemy information for exploitation.

The attack on Pearl Harbor caused the United States Army (Signal Intelligence Service) and Navy to dedicate additional resources to each of their established communications intelligence efforts. Additionally, the attack brought about the refocusing of their efforts from a regional level to a national one.[35] Having implemented many of the lessons learned from Pearl Harbor, the United States was able to change the tide during the Battle of Midway. Information captured before and during the battle gave the United States a tremendous advantage. As a direct result of information obtained, the United States was able to significantly repeal the invasion and attrite Japanese combat power. Nearly sixty years after the attack on Pearl Harbor, the United States experienced another attack on September 11, 2001. Shortly after this attack the intelligence and law enforcement communities determined who the attackers were and subsequently the United States retaliated.

The recent Russo-Georgian and Israeli-Hezbollah conflicts highlight the importance of communication security. During the Russo-Georgian conflict, the Russians allegedly took control of the Georgian news media, financial, and political infrastructure undermining the Georgian government and disrupting their ability to communicate with the people. The cyberspace intelligence preparation of the battlespace (IPB) occurred well in advance of any kinetic rounds destroying targets. Hezbollah claims to have intercepted and exploited Israeli communications during the Israeli-Hezbollah War elevates the potential capabilities of non-state actors. Although this claim is unsubstantiated by the Israelis, it is cause enough for heightened security on the battlefield.

Messengers are indeed the most reliable means to pass information. However, the area of operations and span of command is too great to rely solely on messengers. The cyber domain allows for faster speed, increased access, and more timely information sharing. Operating in cyberspace allows commanders the ability to influence situations before delivering kinetic fires. However, if at any point during a conflict, there is a compromise in communication or the information can no longer be trusted, the battle changes immensely. If foes of the United States are able to monitor or disrupt communications such as global positioning satellites (GPS) or download classified war plans, the ability for aircraft to drop guided munitions or American forces to conduct an amphibious landing could have catastrophic repercussions.

The next step for the United States is to continue to fund and support the established institutions directed to protect the nation and the people. At all levels inside the government, individuals should be educated on the proper and improper use of systems and technologies. Part of this education should also cover historical examples of successes and failures on the battlefield. Commanders must educate themselves on the capabilities that USCYBERCOM has and implement these tools appropriately on the battlefield. In addition, agencies like the National Security Agency should continue developing technologies and systems to protect information while also attempting to exploit similar systems that America's foes utilize.

While the learning environment continues to expand for individuals and governmental agencies earnestly work to retain America's technological superiority, small unit leaders at the fire team, squad, section, platoon, and company levels must culturally change electronic behavior on the battlefield. A specific example of this behavior change is the use of cell phones in theater. Often units use cell phones to communicate with host nations. Cell phones are convenient means to pass information while minimizing risks associated with modern location services (e.g., GPS), software vulnerabilities, and eavesdropping as examples. For years one of the open source methods of tracking Osama bin Laden was the use and reliance of satellites and cell phones by him and his trusted aides. American military leaders must apply these sorts of lessons to minimize unnecessary exposure and vulnerabilities on the battlefield.

Citation and Footnotes

[1] George H. English, *History of the 89th Division, U.S.A.* (Smith-Brooks Printing Company: Denver, CO, 1920), 172.

[2] National Security Agency, *A History of U.S. Communications Secuirty: The David D. Boak Lectures*, July 1973, 9.

[3] *Random House Dictionary* (New York, NY:Random House, Inc., 1966), 298.

[4] Frederick D. Parker, *A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea*, *Midway, and the Aleutians* (Center for Cyptologic History National Security Agency, 1993), 2.

[5] Headquarters U.S. Marine Corps. *Communications and Information Systems*. MCWP 6-22 (Washington, DC: Headquarters U.S. Marine Corps, November 16, 1998), O-15. https://www.doctrine.usmc.mil/signpubs/d10.pdf MCDP 1-0 (accessed February 19, 2012).

[6] George H. English, *History of the 89th Division, U.S.A.* (Smith-Brooks Printing Company: Denver, CO, 1920), 172.

[7] Steven Levy, *Crypto: How the Code Rebels Bea the Government*, *Saving Privacy in the Digital Age* (Penguin Group: Newyork, NY, 2001), 1.

[8] Levy, 346.

[9] Frederick D. Parker, *Pearl Harbor Revisited: U.S. Navy Communications Intelligence 1924-1941* (Center for Cyptologic History National Security Agency, 1994), 4.

[10] Parker, *Pearl Harbor Revisited: U.S. Navy Communications Intelligence 1924-1941*, 19.

[11] Parker, *Pearl Harbor Revisited: U.S. Navy Communications Intelligence 1924-1941*, 20-21.

[12] Parker, *Pearl Harbor Revisited: U.S. Navy Communications Intelligence 1924-1941*, 38-39.

[13] Carl Smith, *Classic Battles: Pearl Harbor 1941 The Day of Infamy* (Botley, Oxford: Osprey Publishing LTD, 1999), 14, 22, 24.

[14] Robert J. Hanyok and David P. Mowry, *West Wind Clear: Cryptology and the Winds Message Controversy-A Documentary History* (Center for Cytologic History National Security Agency, 2008), vii.

[15] George Victor, *The Pearl Harbor Myth: Rethinking the Unthinkable* (Washington, D.C.: Potomac Books, Inc., 2007), 29.

[16.] Hanyok, viii.

[17.] Smith, 9, 32, 90-96.

[18.] Parker, *A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians*, 28-31 and 59-64.

[19.] Parker, *A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians*, 41.

[20.] Ibid.

[21.] Smith, 73.

[22.] Michael Gannon, *Pearl Harbor Betrayed: The True Story of a Man and a Nation under Attack* (New York, NY: Henry Holt and Company, LLC, 2001), 41.

[23.] Ibid.

[24.] Parker, *A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians,* 41.

[25.] National Security Agency, *A History of U.S. Communications Security: The David D. Boak Lectures*, July 1973, 9.

[26.] Smith, 34.

[27.] Smith, 33-38.

[28.] Smith, 39-40.

[29.] Parker, *A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians,* 28-31 and 59-64.

[30.] David Hollis, *Cyberwar Case Study: Georgia 2008*, Small Wars Journal, January 6, 2011.

[31.] Mohamad Bazzi and Sonia Verma, “Hezbollah cracked the code, “ Newsday.com, September 17, 2006, http://www.newsday.com/news/hezbollah-cracked-the-code-1.681121 (accessed on February 22, 2012).

[32.] Ibid.

[33.] Ibid.

[34.] United States Strategic Command. *U.S. Cyber Command Factsheet.* (Omaha, NE: December 2011). http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed March 13, 2012).

[35.] Parker, *Pearl Harbor Revisited: U.S. Navy Communications Intelligence 1924-1941*, 1.

Bibliography

Alverez, David, ed., *Allied and Axis Signals Intelligence in World War II.* Porland, OR: Frank Cass, 1999.

Alvarez, David, *Secret Messages: Codebreaking and American Diplomacy, 1930-1945.* Lawrence, KS: University Press of Kansas, 2000.

Bazzi, Mohamad and Verma, Sonia, "Hezbollah cracked the code, " Newsday.com, September 17, 2006, http://www.newsday.com/news/hezbollah-cracked-the-code-1.681121 (accessed on February 22, 2012) .

Flicke, Wilhem F., *War Secrets in the Ether*. Laguna Hills, CA: Aegean Park Press, 1994.

Gannon, Michael, *Pearl Harbor Betrayed: The True Story of a Man and a Nation under Attack.* New York, NY: Henry Holt and Company, LLC, 2001.

Hanyok, Robert J. and Mowry, David P., *West Wind Clear: Cryptology and the Winds Message Controversy-A Documentary History.* Center for Cytologic History National Security Agency, 2008.

Harper, Stephen, *Capturing Enigma: How HMS Petard Seized the German Naval Codes.* Trowbridge, Wiltshire: Sutton Publishing Limited,1999.

Headquarters U.S. Marine Corps. *Communications and Information Systems*. MCWP 6-22. Washington, DC: Headquarters U.S. Marine Corps, November 16, 1998, O-15. https://www.doctrine.usmc.mil/signpubs/d10.pdf MCDP 1-0 (accessed February 19, 2012).

Haufler, Hervie, *Codebreakers' Victory: How the Allied Cryptographers Won World War II.* New York, NY: New American Library, 2003.

Healy, Mark, *Midway 1942: Turning Point in the Pacific.* Westport, CT: Praeger Publishers, 2004.

Hollis, David, *Cyberwar Case Study: Georgia 2008*, *Small Wars Journal*, January 6, 2011.

English, George H., *History of the 89th Division, U.S.A.* Smith-Brooks Printing Company: Denver, CO, 1920.

Levy, Steven, *Crypto: How the Code Rebels Bea the Government, Saving Privacy in the Digital Age.* Penguin Group: Newyork, NY, 2001.

Merriam-Webster's Collegiate Dictionary: Elevnth Edition. Merriam, Webster, Inc., 2006.

National Security Agency, *A History of U.S. Communications Security: The David D. Boak Lectures*, July 1973.

Parker, Frederick D., *A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians.* Center for Cyptologic History National Security Agency, 1993.

Parker, Frederick D., *Pearl Harbor Revisited: U.S. Navy Communications Intelligence 1924-1941.* Center for Cytologic History National Security Agency, 1994.

Prange, Gordon W., *At Dawn We Slept: The Untold Story of Pearl Harbor.* New York, NY: Penguin Putnam, Inc., 1991.

Random House Dictionary. New York, NY:Random House, Inc., 1966.

Rottman, Gordon L., *World War II Battlefield Communications.* Long Island City, NY: Osprey Publishing Ltd., 2010.

Smith, Carl, *Pearl Harbor 1941: The Day of Infamy.* Botley, Oxford: Osprey Publishing LTD, 1999.

Stille, Mark E., *Midway 1942: Turning Point in the Pacific.* Botley, Oxford: Osprey Publishing LTD, 2010.

Symonds, Criag L., *The Battle of Midway.* Oxford, NY: Oxford University Press, Inc., 2011.

United States Strategic Command. *U.S. Cyber Command Factsheet.* Omaha, NE: December 2011. http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed March 13, 2012).

Victor, George, *The Pearl Harbor Myth: Rethinking the Unthinkable.* Washington, D.C.: Potomac Books, Inc., 2007.